

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

LORETTA WILLIAMS,

Plaintiff,

v.

DDR MEDIA, LLC, *et al.*,

Defendants.

Case No. [22-cv-03789-SI](#)

**ORDER GRANTING DEFENDANT
JORNAYA’S MOTION FOR
SUMMARY JUDGMENT AND
GRANTING ADMINISTRATIVE
MOTION TO SEAL; SEALED
ADDENDUM ATTACHED TO ORDER**

Re: Dkt. Nos. 90, 99

On September 20, 2024, the Court held a hearing on defendant Jornaya’s motion for summary judgment. For the reasons set forth below, the Court GRANTS the motion for summary judgment. The Court also GRANTS the unopposed motion to file under seal at Dkt. No. 99.

BACKGROUND

On June 27, 2022, plaintiff Loretta Williams filed this putative class action lawsuit against defendants DDR Media LLC and Lead Intelligence Inc. d/b/a Jornaya (“Jornaya”). Williams claims that defendants violated her privacy when she visited DDR Media’s website, [snappyrent2own.com](#), because her keystrokes were recorded by a computer code embedded on the website through a Jornaya software product called “TCPA Guardian.” Williams alleges that defendants recorded her personal information and that the recording constitutes wiretapping in violation of California law.

According to Jornaya’s Chief Technology Officer Manny Wald, TCPA Guardian “is designed to help companies comply with the Telephone Consumer Protection Act, or TCPA, which restricts how companies contact consumers using autodialing technology without prior consent.” February 2024 Wald Decl. ¶ 4. Wald states,

The TCPA Guardian service is based on a JavaScript, called LeadiD Create. For a website owner who places LeadiD Create on its website, each time a visitor visits that website, the script generates a unique numerical reference—called a LeadiD—and collects information regarding (1) the website itself; (2) the consent and/or disclosure that was present on the website at the time of the visit; and (3) certain of the visitor’s actions on the website, associating that information with the LeadiD. Specifically, the script captures visitor interactions with fields on the page as well as the page’s visual characteristics and associated labels. This includes any TCPA or other disclosure language present on the website (i.e., seeking the visitor’s consent to receive autodialed calls) as well as the visitor’s act of checking a box near that language (which would indicate his or her consent). Information regarding that interaction would then be assigned to the LeadiD unique to that particular visit.

Id. ¶ 5; *see also* Harlow Decl. Ex. C (Response to Interrogatory No. 1, explaining how TCPA Guardian functions with the “LeadiD Create JavaScript” and stating, *inter alia*, “When a visitor navigates to a page where the script is installed, the script loads and creates a unique LeadiD token that is stored on Jornaya’s servers. As a visitor continues their journey through the lead funnel where the script is implemented, the script witnesses the visitor’s interactions and collects data related to their navigation—including the information about the webpage itself, the consent and/or disclosure that was present on the page at the time of the visit, and certain of the visitor’s interactions with fields or elements on the page—and links it with the same LeadiD token.”).

On or around December 10, 2021, Williams visited DDR Media’s website, snappyrent2own.com. Williams claims that during her visit, TCPA Guardian captured her strokes, clicks and other interactions on the website, including her name, email address, and phone number. Williams alleges that TCPA Guardian is an “eavesdropping software,” and that by using that software, defendants “intentionally tapped the lines of communication” between Williams and DDR Media’s website. Second Amend. Compl. (“SAC”) ¶ 49.

The second amended complaint alleges a single cause of action under California Penal Code § 631(a), the California Invasion of Privacy Act (“CIPA”). That statute penalizes:

Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

or

who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over

any wire, line, or cable, or is being sent from, or received at any place within this state;

or

who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

or

who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

Cal. Penal Code § 631(a) (line breaks added). Williams claims that Jornaya has violated the second prong of the statute because “by using TCPA Guardian, Jornaya willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff and alleged Class Members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.” SAC ¶ 51. Williams alleges that DDR Media is liable under the fourth prong of CIPA because it “partnered” with Jornaya to conduct the illegal wiretapping. *Id.* ¶ 52.

During several rounds of motions to dismiss the complaint, Jornaya argued, *inter alia*, that it did not “read, or attempt to read, or to learn” the contents of any communications because when data is transmitted from websites to Jornaya’s servers through TCPA Guardian, that data is automatically “hashed” and no personally identifiable data or communications are stored on Jornaya’s servers. The Court directed the parties to engage in targeted discovery regarding how TCPA Guardian functions and whether Jornaya “reads, or attempts to read, or to learn” the contents or meaning of electronic communications. The parties engaged in that discovery, and Jornaya has now filed a motion for summary judgment on that issue.

LEGAL STANDARD

Summary judgment is proper if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine dispute as to any material fact and that the movant is entitled to judgment as a matter of law. *See* Fed. R. Civ. P. 56(a). The moving party bears the

1 initial burden of demonstrating the absence of a genuine issue of material fact. *Celotex Corp. v.*
 2 *Catrett*, 477 U.S. 317, 323 (1986). The moving party, however, has no burden to disprove matters
 3 on which the non-moving party will have the burden of proof at trial. The moving party need only
 4 demonstrate to the Court that there is an absence of evidence to support the non-moving party's
 5 case. *Id.* at 325.

6 Once the moving party has met its burden, the burden shifts to the non-moving party to
 7 "designate 'specific facts showing that there is a genuine issue for trial.'" *Id.* at 324 (quoting then
 8 Fed. R. Civ. P. 56(e)). To carry this burden, the non-moving party must "do more than simply show
 9 that there is some metaphysical doubt as to the material facts." *Matsushita Elec. Indus. Co., Ltd. v.*
 10 *Zenith Radio Corp.*, 475 U.S. 574, 586 (1986). "The mere existence of a scintilla of evidence . . .
 11 will be insufficient; there must be evidence on which the jury could reasonably find for the [non-
 12 moving party]." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986).

13 In deciding a summary judgment motion, the Court must view the evidence in the light most
 14 favorable to the non-moving party and draw all justifiable inferences in its favor. *Id.* at 255.
 15 "Credibility determinations, the weighing of the evidence, and the drawing of legitimate inferences
 16 from the facts are jury functions, not those of a judge . . . ruling on a motion for summary judgment
 17" *Id.* However, conclusory, speculative testimony in affidavits and moving papers is insufficient
 18 to raise genuine issues of fact and defeat summary judgment. *Thornhill Publ'g Co., Inc. v. Gen.*
 19 *Tel. & Elec. Corp.*, 594 F.2d 730, 738 (9th Cir. 1979). The evidence the parties present must be
 20 admissible. Fed. R. Civ. P. 56(c)).

21 22 DISCUSSION

23 Jornaya contends that it does not read, attempt to read, or to learn the contents of any of the
 24 information input by a visitor to a website that uses TCPA Guardian because all data entered by the
 25 user, such as a name, is immediately "hashed" as soon as it is transmitted from the website to
 26 Jornaya's servers. Harlow Decl. Ex. C at 4-6 (Response to Interrogatory Nos. 1, 3). Jornaya's CTO
 27 Wald explains the hashing process as follows:
 28

8. As is relevant here, hashing is a process that applies an algorithm to a string of characters of any length to create a fixed-size output made up of a new string of numbers and letters such as 72a40ac74b7a2472826f306f02e508fc.1. This output is called a “hash code” or simply a “hash”. Although the hash code itself is technically purely numeric, it is often represented in hexadecimal notation, which uses both numerals 0-9 and letters A-F to represent numbers 0 through 15.

10. The size of the hash code, i.e., the number of characters, does not depend on the size or number of characters of the input. That is what is meant by creating a hash code of “fixed-sized” output. For instance, the length of a hash code from the input of a single word would be the same as the length of a hash code from the input of an entire dictionary. No matter the input, the output always involves the same number of hexadecimal characters. One therefore cannot deduce the length of the original starting of characters by the length of its hash code.

12. The exact same input that is hashed using the same hashing algorithm will produce the same hash code every time. Conversely, any difference in the input will produce a different hash. This means that “supercalifragilisticexpialidocious” will produce the same hash code each time “supercalifragilisticexpialidocious” is typed in, but “1” and “1.0” will produce entirely different hashes, as will “Main St.” and “Main Street”, or “Samuel Adams” and “Samuel adams”. . . .

13. One of the core benefits of hashing is the ability to validate that two inputs are exactly the same, without having to read, learn, or know what the inputs themselves are. By observing that two hash codes are the same, one can confirm that the two underlying inputs that resulted in those hash codes were the same. In other words, if two hash codes match, then the data that was hashed to create those hash codes is also exactly the same. Moreover, and importantly, unlike encryption that can be decoded with a key, hashing is what is referred to as a “one-way” cryptographic function. There is no “key” that can unlock the hash, nor is there a second algorithm that can be applied to turn the hash code back into the data that originally went into the algorithm. In this way, it is more protective than encryption. Thus, hashing allows you to confirm that the data you have is the data hashed, without “un-hashing” or “reversing” the hash code.

16. TCPA Guardian is most often used by “lead-sellers” and “lead-buyers.” A “leadseller” usually is a company that operates a website that might offer to provide information about a certain product or service (e.g., a mortgage), generating engagement from website visitors. In a typical scenario, the visitor interested in that product or service provides certain information about themselves to the lead-seller on the website in order to receive more information about the products or services advertised. If the lead-seller places the LeadiD Create script on its website, a LeadiD will be generated from the visit, and the hash code of the information provided by the website visitor to the lead-seller is stored by TCPA Guardian and associated with that LeadiD. The lead-seller then sells or provides the LeadiD and certain information provided by the visitor to a “lead-buyer,” which is often the company that offers the actual product or service (e.g., the bank or a broker for mortgages). The lead-buyer uses TCPA Guardian to validate information about the individual who visited the lead-seller’s website, particularly whether the website obtained consent from the visitor to communicate with him or her.

17. TCPA Guardian works as follows: The lead-buyer submits the LeadiD to Jornaya’s TCPA Guardian, along with the hash code for the information it obtained from the lead-seller (e.g., the visitor’s name and telephone number). Jornaya’s TCPA Guardian compares the hash code provided by the lead-buyer to the hash code that TCPA Guardian retained from the visit that originally generated that same

LeadiD—i.e., the hash code for the information that was originally collected when the individual visited the lead-seller’s website. Much like how password hashes are verified, if the hash codes match, then the lead is verified: the data provided by the lead-buyer and the original data collected by the lead-seller are the same. If not, then there is no match. By using a LeadiD as the identifier and storing the hash—and only the hash—of a website visitor’s input, Jornaya can allow lead-buyers to confirm that the data they bought from the lead-seller is indeed the data that a website visitor originally provided to the lead-seller, without Jornaya actually keeping, reading, or learning the original data.

18. This is also why a TCPA Guardian Compliance Report displays asterisks in the place of the visitor’s inputs: Jornaya does not store any of those inputs, including personally identifiable data, and cannot apply any method to reverse the hashes to read the original inputs.

Wald Decl. ¶¶ 8-18. At his deposition, Wald testified that Jornaya automatically performs the hashing of user-inputted data as soon as the data transmitted from the website reaches Jornaya’s servers, and “once the hashing algorithm is applied,” the “original data is discarded” and “is not used” for “any purpose.” Harlow Decl. Ex. A at 27-30 (Wald Depo.). The entire process “occurs within milliseconds.” *Id.* at 27. Wald explained that “[t]he data is received by the server and it is only stored in volatile memory, a RAM, for milliseconds before it is quickly overwritten by other processes, other data, and never stored on any persistent medium.” *Id.* at 28-29.

Williams does not dispute Jornaya’s evidence regarding how the hashing process works. Instead, Williams contends that Jornaya reads, attempts to read, or learns the contents of communications because when Jornaya hashes data, Jornaya first “processes and evaluates” that data by performing select formatting adjustments to the data. Williams cites Wald’s deposition testimony in which he describes how the input is “processed” and “evaluated.” *See* Wald Depo. at 25-26.¹ Williams argues that a jury could reasonably conclude that this initial step of processing and evaluating the input data constitutes “reading” or “attempting to read” or “learning” the contents of the data. Williams also emphasizes that the California Supreme Court has consistently held that CIPA is to be interpreted broadly. *See Ribas v. Clark*, 38 Cal. 3d 355, 359 (1985) (“In enacting [CIPA], the Legislature declared in broad terms its intent to protect the right of privacy of the people of this state from what it perceived as a serious threat to the free exercise of personal liberties that

¹ The parties have agreed that portions of Wald’s deposition testimony in which he explains the technical details of how TCPA Guardian works should be sealed. The Court discusses this testimony in the sealed addendum to this order.

cannot be tolerated in a free and civilized society. This philosophy appears to lie at the heart of virtually all the decisions construing the Privacy Act.”) (internal citations and quotations omitted).

Jornaya argues that in order to “read” or “learn the contents” of a communication under CIPA, there must be some action to interpret or understand the communication’s substantive meaning. Jornaya contends that the undisputed evidence shows that its automated hashing process does not and could not seek to interpret or understand any of the data, and instead that the algorithm makes certain formatting adjustments to the data and then irreversibly transforms it into an incomprehensible alphanumeric string called a hash, all within milliseconds. Jornaya argues that the entire process takes place without the need or capacity for Jornaya to decipher the substantive meaning of the data.

Jornaya asserts that because CIPA does not provide its own definition of “read,” the Court must apply the word’s ordinary meaning. *See DeGeorge v. U.S. Dist. Court*, 219 F.3d 930, 936 (9th Cir. 2000) (“If the statute uses a term which it does not define, the court gives that term its ordinary meaning.”). Jornaya cites dictionary definitions of “read,” such as the Oxford English Dictionary definition of “read,” as “to look over or scan ... with understanding of what is meant by the letters or signs.” Oxford English Dictionary, read, https://www.oed.com/dictionary/read_v?tab=meaning_and_use#26820196 (emphasis added). Jornaya also argues that its interpretation of “read” as requiring gaining some understanding of the communication’s substance is consistent with CIPA’s history and purpose of protecting privacy rights. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020) (“[T]he legislative history and statutory text demonstrate that . . . the California legislature intended to protect . . . historical privacy rights when they passed the . . . CIPA.”); *see also Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022) (“Section 631 was meant to “codi[fy] the common law tort of invasion of privacy.”) (Bumatay, J., concurring).

The Court concludes that the phrase “reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication” in CIPA requires some effort at understanding the substantive meaning of the message, report or communication, and that the evidence shows that TCPA Guardian does not “read, attempt to read, or to learn the contents or meaning” of the

1 information that is input on websites hosting that software. The evidence shows that the data
2 Jornaya receives is automatically subjected to an algorithm that transforms the data into an
3 incomprehensible “hash” that has no inherent substantive meaning, and that Jornaya does not retain
4 the original unhashed data in its servers. The Court is not persuaded by Williams’ argument that
5 the initial step of the hashing process, during which the original data is formatted in a particular
6 way, constitutes “reading” under CIPA. The alteration of the data is an automatic, almost
7 instantaneous step in the hashing process, and does not involve any attempt by Jornaya to understand
8 the substantive meaning of the data.

9 Williams contends that *D’Angelo v. Penny OpCo, LLC*, No. 23-CV-0981-BAS-DDL, 2023
10 WL 7006793 (S.D. Cal. Oct. 24, 2023), supports her position that Jornaya’s software “read” the
11 information that she input on the www.snappyrent2own.com website. In *D’Angelo*, the plaintiffs
12 alleged that JC Penny violated CIPA by permitting a third party, Vergic, to run a chat service on JC
13 Penney’s website. The plaintiffs alleged that when a consumer chatted with a JC Penney customer
14 service representative via the website chat feature, each message was first routed through Vergic’s
15 server, where Vergic would “analyze, interpret, and collect customer-support agent interactions in
16 real time to create live transcripts of communications as they occur.” *Id.* at *1. The district court
17 denied the defendant’s motion to dismiss the complaint, finding that the plaintiffs had sufficiently
18 alleged that JC Penny allowed Vergic “to contemporaneously duplicate their chat conversations
19 with Defendant as they occurred, thereby reading them” and that the plaintiffs had plausibly alleged
20 that JC Penney had violated the second clause of CIPA “by aiding and abetting Vergic, in allowing
21 Vergic to ‘listen in’ on chats between Website users and customer service representatives.” *Id.* at
22 *8-9.

23 Williams’ reliance on *D’Angelo v. Penny OpCo* is unavailing. Unlike Vergic, which
24 allegedly analyzed and interpreted the chat communications to create live transcripts of the
25 communications as they occurred, here the undisputed evidence shows that Jornaya immediately
26 and automatically hashes the input data upon receipt and does not analyze, interpret, or save the
27 original inputted information. *See Gutierrez v. Converse Inc.*, __ F. Supp. 3d __, 2024 WL 3511648,
28 at *7 (C.D. Cal. July 12, 2024) (granting summary judgment to Converse where third party vendor

Salesforce, which provided software to enable chat feature on Converse’s website and stored chats on Salesforce’s servers through password-protected customer dashboard, did not read or attempt to read the chats because the “uncontroverted evidence establishes messages sent through Defendant’s chat feature are encrypted while in transit” and there was no evidence that Salesforce could or did read or attempt to read chats while accessing customer dashboard); *cf. Valenzuela v. Nationwide Mut. Ins. Co.*, 686 F. Supp. 3d 969, 977 (C.D. Cal. 2023) (holding the plaintiff plausibly alleged that third party Akamai read, or attempted to read or to learn the contents of plaintiff’s chat on Nationwide’s website where the plaintiff “alleged that Akamai’s business model is to harvest data from communications” and “Akamai’s business model appears to rely on intercepting all or nearly all messages for mass data analysis.”); *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023) (holding the plaintiff alleged violation of second prong of § 631 by “plead[ing] that ActiveProspect monitors, analyzes, and stores information about visits to Assurance’s websites, and that Active Prospect can use that information for other purposes”).

Williams also provides the following analogy to argue that Jornaya has “read, attempted to read, or learned” the contents of communications:

Perhaps an analogy on this point is a hypothetical scenario of a person receiving a letter in the mail addressed to someone else. The person opens the letter, which is written in English, and—going one word at a time—converts the letter to all uppercase Pig Latin. The person then throws the original letter in the trash can and places the Pig Latin translation in a drawer. The fact that the person only retained the Pig Latin version of the letter does not mean that it didn’t read or learn the contents of the original English letter, if in no other way than in the process of converting the letter into Pig Latin. Applied here, Jornaya intercepted and transmitted to its server Williams’ communications with DDR’s website in its raw form (the English letter), “processed”, “evaluated,” and “altered” it into Pig Latin (the hash code), discarded the original content, and retained the hash. This does not mean that it did not read or learn the contents of the communication. In fact, the opposite is true. It read or learned the content of the communication if at no other point than when it was hashing it.

Opp’n at 11.

Williams’ analogy is inapt. Under that example, the human translator is reading each word and converting each word into a different, albeit nonsensical, word. As Jornaya argues, it may be true that as a matter of human cognition that when a person translates words from one language to another, the person is also interpreting and understanding the words’ meaning. However, based on


1 the Wald declaration and deposition testimony, Jornaya's hashing software automatically and
2 almost instantaneously converts the input data into the hashed data based upon an algorithm. Based
3 upon this record, the Court concludes that TCPA Guardian did not "read, attempt to read, or learn"
4 the contents or message of any communication that Williams input on DDR Media's website. As
5 such, the Court does not reach Jornaya's other arguments in favor of summary judgment.

7 CONCLUSION

8 For the foregoing reasons, the Court GRANTS Jornaya's motion for summary judgment.
9 Because Williams claimed that DDR Media was liable because it partnered with Jornaya in violating
10 CIPA, the Court also grants summary judgment in favor of DDR Media.

11
12 **IT IS SO ORDERED.**

13
14 Dated: November 20, 2024

15 
16 SUSAN ILLSTON
17 United States District Judge
18
19
20
21
22
23
24
25
26
27
28